Request for Proposal

South Dakota Department of Transportation - Office of Air, Rail, and Transit

Asset and Grant Management Software

RFP Number
2863

Software based on specifications and Appendix A, B, C, D, and F

Due August 25, 2022

Primary Contact Information
Contact Name: Monte Meier Telephone Number: 605-773-4169
Email: monte.meier@state.sd.us

Table of Contents

General Information

1.1 Agency Introduction

The State of South Dakota Department of Transportation Office of Air, Rail and Transit (SDDOT) is the direct recipient of Federal Transit Administration (FTA) funding and is responsible for the grant administration of the funds; in addition, to state allocated funds.

1.2 Purpose of Request for Proposal

1.2.1 Background:

SDDOT is requesting vendors of asset and grant management software proposals to assist in the management requirements defined for SDDOT as the administrator and subrecipients of funds related to public transportation.

1.2.2 Goals and Objectives:

Utilize compliant software to manage assets and grants to automate tasks and processes, reduce duplication, increase efficiency, checks and balances, management data, means to communicate with subrecipients and track, monitor due dates, reporting functions, and user friendly. Software must be compliant with FTA regulations such as Transit Asset Management (TAM) National Transit Database (NTD), Transit Award Management System (TrAMS) and grant management.

Regulation References:
Transit Assist Management: https://www.transit.dot.gov/TAM

NTD: https://www.transit.dot.gov/ntd

TrAMS: https://www.transit.dot.gov/funding/grantee-resources/teamtrams/transit-award-management-system-trams

Grant Management: Circular_5010-1E - Revised July 16, 2018 (dot.gov)

200 CFR: https://www.govinfo.gov/app/details/CFR-2011-title34-vol1/CFR-2011-title34-vol1-part299

1.2.3 Description of Components:

- Software program to collect and manage various categories of data pertaining to our vehicles, facilities, and equipment inventory, maintenance, condition, and useful life. Be able to prioritize the vehicles, facilities, and equipment based on rating and useful life in an order of replacement; and to develop a replacement plan based on various data and established criteria, in accordance with federal and state regulations.

- Software program to collect and maintain various categories of data pertaining to federal and state funded grants; capability to manage grant funding, administration, agreements, project monitoring, and funding as well as program compliance through the life a grant in accordance with federal and state regulations.

1.3 Issuing Office and RFP Reference Numbers

The SDDOT Office of Air, Rail and Transit is the issuing office for this document and all subsequent addenda relating to it on behalf of the State of South Dakota. Unless the names of specific agencies are needed for clarity, the term “State” will be used in this RFP to refer to the SDDOT, the Bureau of Information and Telecommunications (“BIT”), other selected State of South Dakota agencies or South Dakota state government as a whole. However, SDDOT will be the coordinating agency for all matters related to any

agreement resulting from this RFP. The reference number for the transaction is RFP# 2863 This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.4 Schedule of Activities (Subject to Change)

RFP publication: 7-21-2022
Deadline for submission of written inquiries: 8-4-2022
Responses to vendor questions: 8-11-2022
Proposal submission: 8-25-2022
Evaluation of proposals to determine short list (if required): 9-1-2022
Demonstrations/presentation/discussions completed (if required): 9-15-2022
Anticipated award decision/contracted negotiation: 10-10-2022

1.5 Submitting Proposal

All proposals must be completed and received at the SDDOT by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and considered ineligible for consideration.

An original of the proposal must be submitted.

The cost proposal must be in a separate sealed envelope and labeled "Cost Proposal".

All proposals must be signed, in ink, by an officer of the Vendor, legally authorized to bind the Vendor to the proposal, and sealed in the form described in this RFP. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP number and title. The words "Sealed Proposal Enclosed" must be prominently denoted on the outside of the shipping container.

Proposals must be addressed and labeled as follows:

REQUEST FOR PROPOSAL #: 2863
PROPOSAL DUE: AUGUST 25, 2022
BUYER: JACK DOKKEN
PROGRAM MANAGER
SOUTH DAKOTA DEPARTMENT OF TRANSPORTATION
700 E BROADWAY AVE
PIERRE SOUTH DAKOTA 57501

All capital letters and no punctuation are used in the address. The address as displayed should be the only information in the address field.

No proposal will be accepted from, or no contract or purchase order will be awarded to any person, firm, or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.6 Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion- Lower Tier Covered Transactions

By signing and submitting a proposal, the Vendor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the Vendor is unable to certify to any of the statements in this certification, the Vendor will attach an explanation to its proposal(s).

1.7 Nondiscrimination Statement

The State requires all contractors, vendors, and suppliers doing business with the State to provide a statement of nondiscrimination. By signing and submitting its proposal(s), the Vendor certifies they do not discriminate in its employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin, or disability.

1.8 Restriction of Boycott of Israel

For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or vendor certifies and agrees that the following information is correct:

The bidder or vendor, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or vendor on this project and terminate any contract awarded based on the bid or response. The successful bidder or vendor further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9 Modification or Withdrawal of Proposals

Proposals may be modified or withdrawn by the Vendor prior to the established due date and time.

No oral, telephonic, or facsimile responses or modifications to informal, formal bids or RFPs will be considered.

1.10 Vendors Inquiries

All written questions should be sent to: monte.meier@state.sd.us only emailed questions will be accepted. Email inquiries must be sent with the subject line “RFP # 2863.

Vendors and their agents (including subcontractors, employees, consultants, or anyone acting on their behalf) may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in 1.4, Schedule of Activities.

The SDDOT prefers to respond to Vendors’ inquiries (if required) via email. Vendors will be notified in the same manner as indicated above regarding any modifications to this RFP. Vendors may not rely on any other statements, either of a written or verbal nature, that alter any specification or other term or condition of this RFP.

Vendors and their agents may not contact the SDDOT regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension or exclusion from specific procurements.

1.11 Proprietary Information

The proposal of the successful Vendor becomes public information. Proprietary information can be protected under limited circumstances, such as client lists and nonpublic financial statements. An entire proposal may not be marked as proprietary. Vendors must clearly identify in the executive summary and the body of the proposal any specific proprietary information they are requesting to be protected. The executive summary

must contain specific justification explaining why the information is to be protected. Also include in the executive summary the following information.

- Firm Name
- Authorized Signature
- Address
- Type or Print Name
- City, State and Zip
- Telephone No
- E-Mail

Proposals may be reviewed and evaluated by any person at the discretion of the SDDOT. All materials submitted become the property of the State and may be returned only at the State's option.

1.12 Presentations/Demonstrations

At its discretion, the State may require a presentation or demonstration by a Vendor to clarify a proposal. However, the State may award a contract based on the initial proposals received without a presentation or demonstration by the Vendor. If presentations or demonstrations are required, they will be scheduled after the submission of proposals. Presentations and demonstrations will be made at the Vendor's expense.

1.13 Discussions

At the State's discretion, the vendor may or may not be invited to have discussions with the State. The discussions can be before or after the RFP has been submitted. Discussions will be made at the vendor's expense.

1.14 Negotiations

This process is a Request for Proposal/Competitive Negotiation process. Each proposal shall be evaluated, and each Vendor shall be available for negotiation discussions and meetings at the SDDOT's request. The SDDOT reserves the right to negotiate on any components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions also will be held as confidential until the award is completed.

1.15 SDDOT Protest Procedures

Section 200.318(k) of Title 2, Code of Federal Regulations, and the common grant rules assign responsibility to the recipient, in accordance with good administrative practice and sound business judgment, for resolving all contractual and administrative issues arising out of their third-party procurements, including, but not limited to, source evaluation, protests, disputes, and claims. FTA will not substitute its judgment for that of the recipient unless the matter is primarily a Federal concern. Violations of law will be referred to the local, state, or Federal authority having proper jurisdiction.

Recipient must have and use documented procurement procedures, consistent with State, local, and tribal laws and regulations and the standards of this section, for the acquisition of property or services required under a Federal award or subaward.

In conformance with FTA Circular 4220.1F, Recipient shall in all instances disclose information regarding any protests to FTA and expeditiously notifying FTA of any protests when applicable. FTA C 4220.1F Ch. VII, (1)(a)(2)(a). All protest decisions must be in writing. FTA C 4220.1F Ch. VII, (1)(a)(1).

Any "Interested Party," as defined in FTA Circular 4220.F, who is aggrieved in connection with the solicitation or award of a contract associated with the FTA grant may protest to the Secretary of the South Dakota Department of Transportation (SDDOT) at 700 East Broadway Avenue, Pierre, South Dakota

57501, or Joel.Jundt@state.sd.us. The protest shall be submitted in writing within ten (10) business days after such aggrieved interested party knows, or should have known, of the facts giving rise thereto. Protests received after the ten-business-day period shall not be considered. The written protest shall include, as a minimum, the following:

A. The name and address of the protestor
B. Appropriate identification of the procurement by bid, RFP, or award number
C. A statement of the reasons for the protest; and,
D. Any available exhibits, evidence or documents substantiating the protest.

Recipient will respond, in detail, to each substantive issue raised in the protest by the protestor. The Secretary of the SDDOT has the authority to make a final determination on the protest. The Secretary's determination will be final. A request for reconsideration of the decision regarding the protest may be allowed by the Secretary of the SDDOT if data becomes available that was not previously known, or there has been an error of law or regulation. FTA will only entertain a protest that alleges SDDOT failed to follow SDDOT'S protest procedures, and the protest must be filed in accordance with FTA'S Third-Party Contracting Guidance Circular (FTA C 4220.1F).

1.16 SDDOT Conflict of Interest Policy

The State's conflict of interest policy is that no employee, officer or agent of the State of South Dakota or approved third party applicant shall participate in the selection, award or administration of a procurement supported by federal funds, if, to his or her knowledge, any of the following has a financial or other interest in suppliers considered for award.

- The employee, officer, or agent
- Any member of his or her immediate family
- His or her partner; or
- An organization, which employs or is about to employ, any of the above, has a financial or other interest in the firm selected for the award.

2.0 Standard Contract Terms and Conditions

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties:

2.1 The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3 of the RFP and by this reference incorporated herein.

2.2 The Contractor's services under this Agreement shall start on date determined by both parties and will be automatically renewed annually, unless terminated sooner pursuant to the terms hereof.

2.3 The Contractor will not use State equipment, supplies or facilities. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

2.4 The State will make payment for services upon satisfactory completion of the services. The TOTAL CONTRACT AMOUNT will be determined after contract negotiation. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL chapter 5-26.

2.5 The Contractor agrees to indemnify and hold the State of South Dakota, its officers, agents and

employees, harmless from and against any and all actions, suits, damages, liability or other proceedings that may arise as the result of performing services hereunder. This section does not require the Contractor to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

2.6 The Contractor, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:
The Contractor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $1 million for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two times the occurrence limit.

B. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
The Contractor agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1 million.

C. Business Automobile Liability Insurance:
The Contractor shall maintain business automobile liability insurance or equivalent form with a limit of not less than $1 million for each accident. Such insurance shall include coverage for owned, hired and non-owned vehicles.

D. Workers' Compensation Insurance:
The Contractor shall procure and maintain workers' compensation and employers' liability insurance as required by South Dakota law.

Before beginning work under this Agreement, Contractor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Contractor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Contractor shall furnish copies of insurance policies if requested by the State.

2.7 While performing services hereunder, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.8 Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third parties, or which may otherwise subject Contractor or the State to liability. Contractor shall report any such event to the State immediately upon discovery.

2.9 Contractor's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Contractor's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

2.10 This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Contractor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. If termination for such a default is affected by the State, any payments due to Contractor at the time of termination may be adjusted to cover any additional costs to the State because of Contractor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this

Agreement. If after the State terminates for a default by Contractor it is determined that Contractor was not at fault, then the Contractor shall be paid for eligible services rendered and expenses incurred up to the date of termination.

2.11 This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of law or federal funds reductions, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

2.12 This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof and be signed by an authorized representative of each of the parties hereto.

2.13 This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

2.14 The Contractor will comply with all federal, state and local laws, regulations, ordinances, guidelines, permits and requirements applicable to providing services pursuant to this Agreement, and will be solely responsible for obtaining current information on such requirements.

2.15 The Contractor may not use subcontractors to perform the services described herein without the express prior written consent of the State. The Contractor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Contractor will cause its subcontractors, agents, and employees to comply, with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.

2.16 Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement shall belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s) and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.

2.17 The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

2.18 Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to State of South Dakota Transit Office on behalf of the State, and by Authorized Designee, on behalf of the Contractor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

2.19 In the event that any court of competent jurisdiction shall hold any provision of this Agreement unenforceable or invalid, such holding shall not invalidate or render unenforceable any other provision hereof.

2.20 All other prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

3.0 Scope of Work

The systems will be cloud solution-based software system with web interface to assist in asset and grant management, analysis, and reporting. The system must also have integration capabilities with other data and reporting systems. This must be a secure system with username and password functionality.

The system must have the capability to allow at a minimum of at least 50-65 external users, with individual log in credentials. The system will have the capability of providing administrator the authority to define user rights and roles.

The system must have functioning standardized reports and queries and have the capability for users to customize reports using system data. Vendor will be required to supply a data dictionary. The system must allow users to customize data collection (field names, form layouts) with no field limitations to meet the administration requirements as processes and requirements change.

Software must be capable of importing data from third party software system programs such as Excel, Access, routing software, or maintenance software to import maintenance records and inspections. The system must be capable to extract reports\data to be used to report enter information into FTA systems such as TrAMS and NTD.

The Vendor will provide an implementation schedule and plan. The Vendor will identify the costs for this service in the cost proposal. As part of the implementation, Vendor will connect data from existing systems to be uploaded into the system to populate system.

The Vendor will provide ongoing technical assistance and support through various means of communication as appropriate to the situation. The Vendor will identify the costs for this service in the cost proposal.

The Vendor will provide detailed and comprehensive training sessions to the SDDOT personnel and external users. The Vendor will identify the costs for this service in the cost proposal.

The Vendor will maintain and provide the user manual. The Vendor will identify the costs for this service in the cost proposal.

The Vendor will provide a one-year warranty service following final system acceptance. After the initial one-year warranty expires, the maintenance agreement will begin. The SDDOT requires the Vendor provide upgrades to ensure the most recent technology is being utilized and new requirements are implemented as required. Costs for this service will be identified in the proposal.

The SDDOT wants to understand the capabilities of the system and any enhancements that are readily built in or could be added in the future. The Vendor will provide a narrative explaining deviations from the specification listed in the RFP. The Vendor is also required to provide a demonstration to showcase the software functionality beyond minimum required specifications.

3.1 Asset Management

Asset management capabilities must be TAM compliant as required by the FTA and provide the following:

(1) Asset inventory (rolling stock, facilities, and equipment)

(2) Condition assessment of assets

(3) Decision support tools

(4) Prioritization of assets based on established criteria

(5) Ridership data collection

(6) Capability of calculating the future useful life and condition of the equipment.

(7) National Transit Database compliant

The system must have the capability to store and analyze data for at least 1,000 vehicles, 100 buildings, 500 individual pieces of equipment and provide the flexibility to handle additional assets as the South Dakota Department of Transportation's ("SDDOT") assets increase. The asset history must be obtained to meet the retention requirements. The system must be easily capable of being updated as technology, as well as program requirements, change over the intended life of the system.

The system will have a task scheduling function to allow users to schedule tasks and notifications based on asset inventory maintenance, reporting, monitoring, and inspection data.

The system will allow users to develop preventive maintenance schedules or inspection forms for each asset based on manufacture recommendation and requirements. The functionality of the system will also capture inspection completed dates, future inspection, and preventive maintenance dates.

Planning and prioritization functions will include the following as a minimum. The below is not an all-inclusive list:

- Entity Information
- Entity Type
- Asset Registry
- Listing of all assets with identifying data
- Asset Maintenance Data (historical and current)
- Preventive, routine, or emergency maintenance records
- Vendor name
- Invoice date
- Invoice number
- Cost payment date
- Amount
- Check number
- Description of work performed
- Odometer or hours reading
- Customizable fields that can be defined by SDDOT
- Asset Condition Data
- Customizable asset scorecard criteria consisting of 5 to 7 categories for vehicle, facilities, and equipment based on SDDOT's Asset Management Plan.
- Proposed Investment Priority List
- Develop replacement plan based on pertinent asset information, maintenance records, and scorecard criteria.
- Capital Improvement Plan analysis and reporting

3.2 Grant Management

Grant management capabilities must be FTA compliant and provide:

(1) Management of funding allocations by year and section of funds

(2) Funding application process for state and subrecipients
(3) Application scoring and ranking, with tools to determine awards based on funds, funding methodology, and application and scoring
(4) FTA grant development and management to submit grants to FTA through the FTA Transit Award Management System (TrAMS)
(5) Funding Agreement development, monitoring, closeout, and retention
(6) Procurement process tracking (internal and external)
(7) Grant funding awards and expenditure tracking (external)
(8) Upload documentation capabilities with a filing structure
(9) Management reimbursement requests and voucher processing (expenditures)
(10) Reconciliation features to reconcile with finance and FTA
(11) Data collection, management, and reporting
(12) Program monitoring tools
(13) Task management (internal and external)
(14) Electronic signature capabilities
(15) Project Monitoring (Monitor various steps throughout the life of the life with monitoring tool, status updates and closeouts.)
(16) Vehicle ordering process (order form, purchase orders, notice to proceed, inspection documents)

The system must have the capability to store and analyze data for all grants related to transit (could be up to 50 grants) and provide the flexibility to handle additional types of grants as the South Dakota Department of Transportation's ("SDDOT") grant opportunities increase. The grant history must be obtained to meet the retention requirements. The system must have the capability of being updated as technology, as well as program requirements, change over the intended life of the system.

The system will have a task scheduling and notification function to allow users to schedule tasks based on their grant requirements such as due dates, reporting, reimbursement requests, project status updates, procurement tracking, and grant allocations and expenditures. The system will also have the capabilities to enable the SDDOT to assign tasks to the external users.

The system will give users the tools to provide grant administration, and project management\monitoring for each grant based on requirements for internal and external tasks.

Planning and Prioritization functions will include the following as a minimum. The below is not an all-inclusive list:

- Grant Registry
    - Listing of all grants with identifying data
    - Track Apportionments
    - Performance data
- Grant Invoice Processing
    - Entity Information
    - Unique Identifying Information
    - Vendor Name
    - Invoice date
    - Invoice number
    - Cost Payment date

        - Amount
        - Check number
        - Description of what was purchased
        - Agreement Number
        - Federal and local amounts
    - Grant Status Data
        - Track Grants through FTA's TrAMS system.
        - Track agreements with sub-recipient
        - Track and set up project numbers
    - Reporting
        - NTD Reporting capabilities
        - STIP report
        - Project Tracking
        - Milestone Report
        - Charter Reporting
        - DBE Reporting
    - Process applications
        - Prepare application
        - Review application
        - Determine Award
        - Prepare Program of Projects (POP)
        - Prepare narrative for TrAMS
    - Proposed Investment Priority List

      Develop award plan based on pertinent asset information, financial records, and scorecard criteria.

3.3 Hosting and Data Access Requirements

The contract doubles as an agreement for the State to own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data, and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms. Refer to Appendix A-2

3.4 Single Sign-On Requirements

As part of the State's Identity and Access Management (IAM) strategy, the proposed solution will need to integrate with the State of South Dakota's standard identity management service single sign-on (SSO) which enables custom control of how citizens and state employees sign up, sign in, and manage their profiles.

The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users.

If the vendor is not able to fulfil this identity management standard they will be excluded from the list

3.5 Interfaces and Integration

The vendor must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, SDDOT expects that the vendor will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability shall be included in the proposal.

4.0 Project Deliverables/Approach/Methodology

If the vendor is hosting the solution, provide a diagram giving an overview of the proposed system. It is preferred that this diagram be provided as a separate document or attachment. The file must be named "(Your Name) Hosted System Diagram". If the vendor elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

The vendor should state whether its proposed solution will operate in a virtualized environment. Vendor also should identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment. This information must be included with the solution diagram for the vendor hosted solution.

This section identifies tasks and deliverables of the project as described in Section 3 above. The selected vendor is responsible for providing the required deliverables. These deliverables will be the basis against which the vendor's performance will be evaluated.

The vendor is required to include a test system for its application. This test system will be used at the discretion of BIT. All resource costs associated with keeping the test system available must be borne by the project owner or the vendor. Any licensing costs for the test system must be included with the costs.

At BIT's discretion, any code changes made by the vendor, either during this project or thereafter, will be placed in the above test system first. It is at BIT's discretion if the code changes are applied by BIT or the vendor. If the code testing delays a project's timeline, a change management process should be followed, and the State will not be charged for this project change. If the test and production systems are to be hosted by the State, the schedule for the testing of the code changes is to be decided by BIT. Testing of emergency code changes will be scheduled by BIT based on the severity and resource availability.

The test system will be maintained by the vendor as a mirror image of the production system code base. At BIT's discretion, updates to the production system will be made by copying code from the test system after the test system passes BIT certification requirements.

If BIT determines that the application must be shut down on the production system, for any reason, the vendor will, unless approved otherwise by BIT, diagnosis the problem on and make all fixes on the test system. The vendor is expected to provide proof, to BIT, of the actions taken to remediate the problem that lead to the application being denied access to the production system before the application can go back into production. This proof can be required by BIT even if the fix passes all BIT certification criteria. BIT is willing to sign a non-disclosure agreement with the vendor if the vendor feels that revealing the fix will put the vendor's intellectual property at risk.

All solutions acquired by the State that are hosted by the vendor, including Software as a Service, or hosted by a third-party for the vendor will be subjected to security scans by BIT or preapproved detailed security scan report provided by the vendor. The scan report sent in with the proposal can be redacted by the vendor. The State's goal at this point is to see if the contents of the report will be acceptable, not to review the contents themselves. If the vendor will be providing a security scan report, one must be sent with the proposal for approval. Approval is not guaranteed. If the scan report is not acceptable, the State must scan the vendor's solution. The actual scanning by the State or the submission of a security scan report will be done if the proposal is considered for further review. A detailed security report must consist of at least:

- The system that was evaluated (URL if possible, but mask it if needed).
- The categories that were evaluated (example: SQL injection, cross site scripting, etc.)
    - What were the general findings, (meaning how many SQL injection issues were found, what was the count per category)
    - Technical detail of each issue found. (where was it found – web address, what was found, the http response if possible)

The cost of any scans done by the vendor or the vendor's costs associated with the State's scans must be part of the vendor's bid. If the vendor is sending a security scan report, it should price the product both as if the State was to do the security scan or if the vendor was to do the security scan.

Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing. If the State determines the hardware, website(s), software, and or cloud services have security vulnerabilities that must be corrected, the State will inform the vendor of the nature of the issue and the vendor will be required to respond in writing regarding mitigation plans for the security vulnerabilities. If the product(s) does not pass the initial security scan, additional security scans may be required to reach an acceptable level of security. The vendor must pass a final follow-up security scan for the website(s), software, or cloud services for the product(s) to be acceptable products to the State. The State may suspend or cancel payments for hardware, website(s), software, or cloud services that do not pass a final security scan.

Any website or web application hosted by the vendor that generates email cannot use "@state.sd.us" as the originating domain name per state security policy.

If the vendor is proposing to use a web application or provide Software as a Service, the most current version of Active Directory Federation Service (ADFS) will be used for all user logins for State of South Dakota staff, if supported by the vendor. If the vendor cannot make use of ADFS, the vendor must explain how State staff will be informed not to use their State password to login to the vendor's solution.

As part of this project, the vendor will provide a monitoring tool the State can utilize to monitor the operation of the proposed solution as well as all systems and all subcomponents and connections. It is required that this tool be easy to use and provide a dashboard of the health of the proposed solution. The effectiveness of this monitoring tool will be a component of the acceptance testing for this project.

As part of the project plan, the vendor will include development of an implementation plan that includes a back out component. Approval of the implementation plan by BIT should be a project milestone. Should the implementation encounter problems that cannot be resolved and the implementation cannot proceed to a successful conclusion, the back out plan will be implemented. The Implementation and back out documentation will be included in the project documentation.

The successful vendor will use the approved BIT processes and procedures when planning its project, including BIT's change management process. Work with the respective agency's BIT Point of Contact on this form. The Change Management form is viewable only to BIT employees. The purpose of this form is to alert key stake holders (such as: Operations, Systems Support staff, Desktop Support staff, administrators, Help Desk personnel, client representatives, and others) of changes that will be occurring within state resources and systems to schedule the:

- Movement of individual source code from test to production for production systems
- Implementation of a new system
- A major enhancement to a current system or infrastructure changes that impact clients
- Upgrades to existing development platforms

If as part of the project the state will be acquiring software the proposal should clearly state if the software license is perpetual or a lease. If both are options, the proposal should clearly say so and state the costs of both items separately.

Include in your submission details on your:

- Data loss prevention methodology;
- Identity and access management;
- Security intelligence;
- Annual security training and awareness;
- Manual procedures and controls for security;

- Perimeter controls;
- Security certifications and audits.

If the vendor will have State data on its system(s) or on a third-party's system and the data cannot be sanitized at the end of the project, the vendor's proposal must indicate this and give the reason why the data cannot be sanitized as per the methods in NIST 800-88.

The vendor's solution cannot include any hardware or hardware components manufactured by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State's network as well as the vendor's network if the vendor's network is accessing the State's network or accessing State data. This includes Infrastructure as a Service, Platform as a Service or Software as a Service situations. Any company that is considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act, in a United States appropriation bill, an Executive Order, or listed on the US Department of Commerce's Entity List will be included in this ban.

If the vendor's solution requires accounts allowing access to State systems, then the vendor must indicate the number of the vendor's staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State's costs in providing these accounts will be a consideration when assessing the cost of the vendor's solution. If the vendor later requires accounts that exceed the number of accounts that was originally indicated, the costs of those accounts will be borne by the vendor and not passed onto the State. All State security policies can be found in the Information Technology Security Policy (ITSP) attached to this RFP. The vendor should review the State's security policies regarding authorization, authentication, and, if relevant, remote access (See ITSP 230.67, 230.76, and 610.1). Use of Remote Access Devices (RAD) by contractors to access the State's system must be requested when an account is requested. The vendor should be aware that access accounts given to non-state employees, Non-State (NS) accounts, will be disabled if not used within 90 days. A NS account will be deleted after 90 days if it is not used.

If the vendor's solution requires State staff to log-in, then the vendor should indicate if its solution can use the State's Active Directory to provide single-sign-on.

Integration Testing- Integration testing is a software development process which program units are combined and tested as groups in multiple ways. In this context, a unit is defined as the smallest testable part of an application. Integration testing can expose problems with the interfaces among program components before trouble occurs in real-world program execution. Integration testing is also known as integration and testing (I&T).

Functional Testing- Functional testing is primarily used to verify that a piece of software is meeting the output requirements of the end-user or business. Typically, functional testing involves evaluating and comparing each software function with the business requirements. Software is tested by providing it with some related input so that the output can be evaluated to see how it conforms, relates or varies compared to its base requirements. Moreover, functional testing also checks the software for usability, such as ensuring that the navigational functions are working as required. Some functional testing techniques include smoke testing, white box testing, black box testing, and unit testing.

User Acceptance Testing -User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications. UAT is one of the final and critical software project procedures that must occur before newly developed or customized software is rolled out. UAT is also known as beta testing, application testing or end user testing. In some cases, UAT may include piloting of the software.

The State, at its sole discretion, may consider a solution that does include all or any of these deliverables or consider deliverables not originally listed. An vendor **must** highlight any deliverable it does not meet and give any suggested "work-around" or future date that it **will** be able to provide the deliverable.

5.0 Format of Submission

The Vendor must submit an original of each proposal.

All proposals should be prepared simply and economically and provide a direct, concise explanation of the vendor's proposal and qualifications. Elaborate brochures, sales literature and other presentations unnecessary to a complete and effective proposal are not desired.

The vendor is cautioned that it is the vendor's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The vendor's failure to submit such information may cause an adverse impact on the evaluation of the proposal. The vendor must respond to each point in the Scope of Work and Deliverables in the order they were presented.

Vendors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all questions or comments regarding the RFP or the evaluation to the buyer of record indicated on the first page of this RFP. Vendors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and exclusion from specific procurements. Vendors and their agents who have questions regarding this matter should email the buyer of record at monte.meier@state.sd.us.

The vendor may be required to submit a copy of its most recent audited financial statements upon the State's request.

The proposal should be page numbered and should have an index or a table of contents referencing the appropriate page number. Each of the sections listed below should be tabbed.

Vendors are cautioned that use of the State Seal in any of their documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

Proposals should be prepared using the following headings and, in the order that they are presented below. Please reference the section for details on what should be included in your proposal.

5.1 Executive Summary

The one or two-page executive summary will briefly describe the Vendor's proposal. It must identify any requirements that cannot be met by the Vendor. A reader should be able to ascertain the essence of the proposal by reading the executive summary. Proprietary information requests should be stated here.

5.2 Statement of Understanding of Project

To demonstrate your comprehension of the project, the vendor should summarize their understanding of what the work is and what the work will entail. This should include, but not be limited to, the vendor's understanding of the purpose and scope of the project, critical success factors and potential problems related to the project, and the vendor's understanding of the deliverables. The vendor should include their specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements. This section should be limited to no more than two pages.

5.3 Corporate Qualifications

Provide responses to the each of the following questions in your proposal.

A. What year was your parent company (if applicable) established?

B. What is the business of your parent company?

C. What is the total number of employees in the parent company?

D. What are the total revenues of your parent company?

E. How many employees of your parent company have the skill set to support this effort?

F. How many of those employees are accessible to your organization for active support?

G. What year was your firm established?

H. Has your firm ever done business under a different name and if so what was the name?

I. How many employees does your firm have?

J. How many employees in your firm are involved in this type of project?

K. How many of those employees are involved in on-site project work?

L. What percent of your parent company's revenue (if applicable), is produced by your firm?

M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project

N. Availability to the project locale

O. Familiarity with the project locale

P. Has your firm ever done business with other governmental agencies? If so, please provide references.

Q. Has your firm ever done business with the State of South Dakota? If so, please provide references.

R. Has your firm ever done projects that are like or similar to this project? If so, how many clients are using your solution? Please provide a list of four or more locations of the same approximant nature as the State where your application is in use along with contact names and numbers for those sites. The State of South Dakota has a consolidated IT system. **Either** any references given should be from states with a consolidated IT system, to be acceptable **or** the reference should be a detailed explanation on how you will modify your work plan for a consolidated environment that you are unfamiliar with.

S. Provide the reports of third-party security scans done at the end of the four projects you provided in your proposal response. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies or tools that has been run within the past 90 days. The State will sign a non-disclosure agreement, as needed, and redaction of these scan reports can be done within the limits of the State's open records law.

T. What is your Company's web site?

When providing references, the reference must include the following information:

- Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted
- Dates of the service/contract
- A brief, written description of the specific prior services performed and requirements thereof

5.4 Relevant Project Experience

Provide details about four recent projects that the vendor was awarded and then managed through to completion. Project examples should include sufficient detail so the agency fully understands the goal of the project; the dates (from start to finish) of the project; the vendor's scope of work for the project; the responsibilities of the vendor and subcontractors in the project; the complexity of the vendor's involvement in the project; deliverables provided by the vendor; the methodologies employed by the vendor; level and type of project management responsibilities of the vendor; changes that were made and request for changes that differed from the onset of the project; how changes to the project goals, vendor's scope of work, and deliverables were addressed or completed; price and cost data; quality of the work and the total of what the vendor accomplished in the project.

A. Client/Company Name
B. Client Company Address, including City, State and Zip Code
C. Client/Company Contacts(s)
    i. Name
    ii. Title
    iii. Telephone Number
    iv. E-mail address
    v. Fax Number
D. Project Start Date
E. Project Completion Date
F. Project Description and Goals
G. Vendor's Role in Project
H. Vendor's responsibilities
I. Vendor's Accomplishments
J. Description of How Project Was Managed
K. Description of Price and Cost Data from Project
L. Description of special project constraints, if applicable
M. Description of your ability and proven history in handling special project constraints
N. Description of All Changes to the Original Plan or Contract That Were Requested
O. Description of All Changes to the Original Plan or Contract That Vendor Completed
P. Description of How Change Requests Were Addressed or Completed by Vendor
Q. Was Project Completed in a Timeframe That Was According to the Original Plan or Contact? (If "No", provide explanation)
R. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

S. Was there any Litigation or Adverse Contract Action regarding Contract Performance? (If "Yes" provide explanation)

T. Feedback on Vendor's Work by Company/Client

U. Vendor's Statement of Permission for the Department to Contact the Client/Company and for the Client's/Company's Contract(s) to Release Information to the Department

5.5 Assessment of Work

A complete narrative of the Vendor's assessment of the work to be performed, the Vendor's ability and approach, and the resources necessary to fulfill the requirements; demonstrating the Vendor's understanding of the desired overall performance expectations.

5.6 Project Plan

The responsibilities and schedule for performing the work. The Vendor will provide a project plan that indicated how the Vendor will complete the required deliverables and services and addresses the following:

- Proposed project management techniques;
- Number of Vendor's staff needed;
- Tasks to be performed (within phase as applicable);
- Number of hours each task will require;
- Deliverables created by each task;
- Dates by which each task will be completed (dates should be indicated in terms of elapsed time from project inception);
- Resources assigned to each task;
- Required State agency support;
- Show task dependencies; and
- Training (if applicable)

Microsoft Project is the standard scheduling tool for the State of South Dakota. The schedule should be a separate document, provided in Microsoft Excel, and submitted as an attachment to your proposal.

If, as part of the project, the Vendor plans to set-up or configure the software or hardware and plans to do this outside of South Dakota, even in part, then the Vendor needs to provide a complete and detailed project plan on how the Vendor plans on migrating to the State's site. Failure to do so is sufficient grounds to disregard the Vendor's submission, as it demonstrates the Vendor fundamentally does not understand the project. Providing a work plan for the steps identified in this section that is complete and detailed may be sufficient.

5.7 Deliverables

This section should constitute the major portion of the work to be performed. Provide a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the vendor's ability to fulfill the requirements of this RFP, the vendor's approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale and a description of any options or alternatives proposed. This should demonstrate that the vendor understands the desired overall performance expectations. This response should identify each requirement being addressed as enumerated in section 8. If you have an alternative methodology or deliverables you would like to propose, please include a detailed description of the alternative methodology or deliverables and how they will meet or exceed the essential requirements of the methodology and deliverables described in Section 4.

5.8 Non-Standard Hardware and Software

State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware or software, you must first obtain State approval. If your proposal recommends using non-standard hardware or software, the proposal should very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use non-standard hardware or software to complete the project requirements. The use of non-standard hardware or software requires use of the State's New Product Process. This process can be found through the Standards' page and must be performed by State employees. The costs of such non-standard hardware or software should be reflected in your cost proposal. The work plan should also account for the time needed to complete the New Product Process. See http://bit.sd.gov/standards/, for lists of the State's standards. The proposal should also include a link to your hardware and software specifications.

If non-standard hardware or software is used, the project plan and the costs stated in 8.7 must include service desk and field support, since BIT can only guarantee best effort support for standard hardware and software. If any software development may be required in the future, hourly development rates must be stated. The project plan must include the development and implementation of a disaster recovery plan since non-standard hardware and software will not be covered by the State's disaster recovery plan. This must also be reflected in the costs.

The vendor must complete the list of technical questions, Security and Vendor Questions which is attached as Appendix B. These questions and the vendor's responses may be used in the proposal evaluation.

5.9 System Diagram

If not a separate document: Provide according to Section 5 of RFP.

5.10 Contract terms acceptability

The Vendor will comply with BIT's standard contract terms and conditions attached to this RFP as **Appendix A** and incorporated into this RFP by reference. The Vendor will submit a statement indicating the acceptability of BIT's technology-specific standard contract terms and conditions, attached to this RFP as **Appendix A**.

Include explanations of any unacceptable provisions;
The Vendor will comply with the State's standard contract terms and conditions in Section 2 of this RFP. A statement indicating the acceptability of State's standard contract terms and conditions. Include explanations of any unacceptable provisions; and any agreement resulting from this RFP will include BIT's terms and conditions listed in Appendices A and F, along with any additional contract terms as negotiated by the parties. As part of the negotiation process, the contract terms listed in RFP may be altered or deleted with the approval of the State. The Vendor should indicate in the Vendor's response, any issues the Vendor may have with specific contract terms. If the Vendor does not indicate there are any issues with any contact term, then the State will assume those terms are acceptable to the Vendor.

5.11 Security Acknowledgement

The Vendor will comply, and sign BIT's Security Acknowledgment Form attached to this RFP as **Appendix D.**

5.12 BIT Security and Vendor Questions Form

Attached to this RFP as Appendix B. The Vendor will answer and complete the BIT security and vendor questions form attached to this RFP as **Appendix B** and incorporated into this RFP by reference.

5.13 Cost Proposal

A detailed description of: any one-time charges, annual fees, any per-user fees for technical requirements listed in this RFP, and additional options offered by the Vendor. A sample cost proposal is attached to this RFP as stated in Section 5 of RFP. The Vendor may be expected to perform additional work as required by

any of the State signatories to the agreement. This work can be made a requirement by the State for allowing the application to go into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies, or excessive resource consumption. The Vendor should include the cost for additional work in the Vendor's proposal.

5.14 Professional References

Information related to recent or current contracts performed by the Vendor's organization, similar to the requirements of this RFP, including:

5.14.1 Client/Company name, Client/Company address, Client/Company Name of contact(s) and title(s), email address and telephone number of the client contacts who can be contacted for all information submitted;
5.14.2 Statement of permission for the SDDOT to contact the clients and for the clients' contact(s) to release information to the SDDOT;
5.14.3 Contract dates; and
5.14.4 A brief written description of the services performed and the solutions provided for the clients, including timelines of project start dates and production dates of each fully operational module of Electronic Performance Support Systems (EPSS) software.

6.0 Cost Proposal

Cost will be evaluated independently from the technical proposal. Vendors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

The vendor must submit a statement in the Proposal that attests the vendor's willingness and ability to perform the work described in this RFP for the price being offered.

6.1 Staffing

Name	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

6.2 Travel and Expenditure Table

Name	Method of Travel	Cost per trip	Number of Trips	Total Cost
			Total:	

Name	Lodging Cost per night	Number of Nights	Lodging Cost	Per diem	Number of Days	Per diem Cost	Total Cost
Totals:							

NOTE: The State asks that vendors accept state per diem. Lodging and per diem rates can be found at https://bhr.sd.gov/files/travelrates.pdf.

6.3 Other Costs

Show any other costs such as: software, hardware, ongoing costs, etc.

	One Time	Year 1	Year 2	Year 3	Totals
Hardware					
Software					
Maintenance					
License Fees					
Training					
Other…					
Totals					

6.4 Additional Work

The vendor may be expected to perform additional work as required by any of the State signatories to a contract. This work can be made a requirement by the State for allowing the application to go into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies, or excessive resource consumption. The cost for additional work should be included in your proposal.

7.0 PROPOSAL EVALUATION AND AWARD PROGRESS

7.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) shall use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria:

7.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;

- Software meets the required minimum specifications
- Additional transit related modules
- Functions beyond minimum specifications
- BIT evaluation and testing results
- Responsive and Responsible Vendor
- Cost:
  - Initial software costs
  - Implementation associated costs
  - Training associated costs
  - Breakdown of User fees
  - Maintenance fees
  - Technical support fees
  - Enhancement costs

7.1.2 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

7.1.3 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

7.1.4 Availability to the project locale;

7.1.5 Familiarity with the project locale;

7.1.6 Proposed project management techniques; and

7.1.7 Ability and proven history in handling special project constraints

7.2 Experience and reliability of the responder's organization are considered subjectively in the evaluation process. Therefore, the responder is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

7.3 The qualifications of the personnel proposed by the responder to perform the requirements of this RFP, whether from the responder's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the responder should submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

7.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

7.5 **Award:** The requesting agency and the highest ranked responder will mutually discuss and refine the scope of services for the project and will negotiate terms, including compensation and performance schedule.

8.0 Best and Final Offers

The State reserves the right to request best and final offers. If so, the State will initiate the request for best and final offers; best and final offers may not be initiated by a vendor. Best and final offers may not be necessary if the State is satisfied with the proposals received.

If best and final offers are sought, the State will document which vendors will be notified and provide them opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the request for proposals and instructions contained in the request for best and final offer. If a vendor does not submit a best and final offer or a notice of withdrawal, the vendor's previous proposal will be considered that vendor's best and final proposal. After best and final offers are received, final evaluations will be conducted.

Appendixes

State of South Dakota Bureau of Information and Telecommunications (BIT) Standard Contract Terms and Conditions

State of South Dakota

BIT Standard State Technology Contract Terms

PROVISION OF DATA

Upon notice of termination by either party, the State will be provided by the Consultant all current State Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Consultant with all current State Data in a non-proprietary form. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

THREAT NOTIFICATION

Upon becoming aware of a credible security threat with the Consultant's product(s) and or service(s) being used by the State, the Consultant or any subcontractor supplying product(s) or service(s) to the Consultant needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Consultant will provide the State with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Consultant.

ADVERSE EVENT

The Consultant shall notify the State Contact within 24 hours if the Consultant becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. If the Adverse Event was the result of the Consultant's actions or inactions. The State can require a risk assessment of the Consultant the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

The Consultant also acknowledges that if not kept secure, the State's data could be, in aggregate, used for illegal purposes.

Except as mandated by other legal requirements the Consultant shall provide notice of the disclosure only to the State. Notification to the State of an Adverse Event involving the disclosure of State Data shall consist of:

i. a description of the data disclosed;
ii. the time the disclosure occurred, and;
iii. a general description of the circumstances of the disclosure.

If all this information is not available for the notification within the specified time, the Consultant shall provide the State with all the available information along with the reason for the incomplete notification.

The parties agree with respect to any Adverse Event that the Consultant shall at its sole expense:

i. promptly and fully investigate the cause of the Adverse Event;
ii. cooperate fully with the State's investigation of, analysis of, and response to the incident;
iii. Take all reasonable steps to mitigate any harm caused to affected individuals and/or entities and to prevent any future reoccurrence;
iv. provide the State with documentation of responsive actions taken related to the disclosure, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement, and;
v. comply with applicable data breach notification laws, including without limitation the provision of credit monitoring and other fraud prevention measures, for a period of ____ _____ months from the date that Consultant notifies Customer of the Adverse Event

The State will determine if notification to individuals or entities other than the State is required and if the notification will be carried out by the State or by the Consultant. The method and content of the notification of the affected parties will be subject to approval by the State.

At the State's discretion and at the Consultant's expense the Consultant may be required to use a credit monitoring service, call center, and/or a forensics company.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Consultant will reimburse the State in full for all costs incurred by the State in the notification, investigation and remediation of the disclosure.

BROWSER

The system, site, and/or application must be compatible with vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion and Adobe Flash will not be used in the system, site, and/or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

INFORMATION TECHNOLOGY STANDARDS

Any service, software or hardware provided under this agreement will comply with state standards which can be found at *http://bit.sd.gov/standards/* .

ACCEPTABLE PROGRAMMING LANGUAGES

The application(s) covered in this contract are_____. All applications listed will be written in C#, and use ASP.NET, MVC, UWP, or WPF.

PRODUCT SUPPORT

The State will install and operate the Consultant's product on the State's computing infrastructure. The State will not be responsible for added support costs if the Consultant determines that the Consultant is unable to meet the support commitment(s) given by the Consultant in this agreement. Any additional costs for support will be borne by the Consultant.

PRODUCT USAGE

The State cannot be held liable for any additional costs or fines for mutually understood product usage over and above what has been agreed to in this Agreement unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

SECURITY

The Consultant shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this agreement, the Consultant warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:
    a. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
    b. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
    c. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
    d. **Low-** Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.
B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.
C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.
D. All members of the development team have been successfully trained in secure programming techniques.

E. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.
F. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at http://bit.sd.gov/standards/.
G. The Consultant will fully support and maintain the Consultant's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Consultant may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Consultant's application to a new release of third-party technology if:
    i. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
    ii. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Consultant may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.
If a code base or platform on which the Consultant's application depends is no longer supported, maintained, or patched by a qualified third party the Consultant commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Consultant to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

LICENSE TO PERFORM SECURITY SCANNING

Before acceptance by the State the Consultant will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or the Consultant has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the state security scanning efforts discover security issues, the State may collaborate, at the State's discretion, with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Consultant. The State will not be charged for any costs incurred by Consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

SECURITY SCANNING

The State routinely applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Consultants who do business with the State must also subscribe to industry security practices and requirements. Consultants must include costs and time needs in their proposals and project plans to assure they can maintain currency with all security needs throughout the lifecycle of a project. The State will collaborate in good faith with the Consultant to help them understand and support State security requirements during all phases of a project's lifecycle but will not assume the costs to mitigate applications or processes that fail to meet then-current security requirements.

At the State's discretion, security scanning will be performed and or security settings put in place or altered during the software development phase and during pre-production review for new or updated code. These scans and tests, initially applied to development and test environments, can be time consuming and should be accounted for in project planning documents and schedules. Products not meeting the State's security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the State's satisfaction. The discovery of security issues during UAT are automatically sufficient grounds for non-acceptance of a product even though a product may satisfy all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Consultant producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

SECURE PRODUCT DEVELOPMENT

By signing this agreement, the Consultant agrees to provide the following information to the State:

A. Name of the person responsible for certifying that all deliverables are secure.
B. Documentation detailing the Consultant's version upgrading process.
C. Notification process for application patches and updates.
D. List of tools used in the software development environment used to verify secure coding.
E. Based on a risk assessment, provide the State the secure configuration guidelines, specifications and requirements that describe security relevant configuration options and their implications for the overall security of the software. The guidelines, specifications and requirements must include descriptions of dependencies on the supporting platform, including operating system, web server, application server and how they should be configured for security. The default configuration of the software shall be secure.

At the State's discretion the State will discuss the security controls used by the State with the Consultant upon the Consultant signing a non-disclosure agreement.

MALICIOUS CODE

A. The Consultant warrants that the software contains no code that does not support an application requirement.
B. The Consultant warrants that the software contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the software or any media on which the software is delivered any malicious or intentionally destructive code.
D. The Consultant warrants that the Consultant will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the software before installation. In the event any malicious code is discovered in the software delivered by the Consultant, the Consultant shall provide the State at no charge with a copy of the applicable software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION

During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended while the application and or hardware is denied access to or removed from production. The reasons can be because of the Consultant's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval. It is expected that the Consultant shall provide the State with proof of the safety and or effectiveness of the remedy, update or patch proposed before the State provides access to the production system. The State shall sign a non-disclosure agreement with the Consultant if revealing the update or patch will put the Consultant's intellectual property at risk. If the remedy, update or patch the Consultant proposes is unable to present software and or hardware that meets the State's requirements, as defined by the State, which may include but not limited to security, functionality, unsupported third party technologies, to the State's satisfaction within thirty (30) days of the denial of access to or removal from the production system and the Consultant does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State's discretion the Agreement may be terminated.

MOVEMENT OF PRODUCT

The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Consultant within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. As part of normal operations, the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and usage restrictions outlined elsewhere in the Agreement. All such movement of product can be done by the State without any additional fees or charges by the Consultant.

USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE

The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product shall be the only consideration in licensing compliance related to computing resource capacity.

LOAD BALANCING

The State routinely load balances across multiple servers, applications that run on the State's computing environment. The Consultant's product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Consultant's product to be load balanced so that it can operate on the State's computing environment will be at the Consultant's expense.

BACKUP COPIES

The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:

A. The State maintains possession of the backup copies.
B. The backup copies are used only as bona fide backups.

USE OF ABSTRACTION TECHNOLOGIES

The Consultant's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Consultant warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Consultant and will not be a project change chargeable to the State. If the use of hard-coded references is

discovered after User Acceptance Testing the Consultant will correct the problem at no additional cost.

LICENSE AGREEMENTS

Consultant warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

WEB AND MOBILE APPLICATIONS

The Consultant's application is required to;

A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
C. close all connections and close the application at the end of processing;
D. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
E. have no code not required for the functioning of application;
F. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
G. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
I. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
J. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Consultant's application;
K. access no data outside what is defined in the "About" information for the Consultant's application;
L. your web site application produced for the State must conform to Web Content Accessibility Guidelines 2.0;
M. any website developed for the State and hosted by the State must have a Single Sign On capability with the State's other websites; and
N. any application to be used on a mobile device must be password protected.

The Consultant is required to disclose all:

A. functionality;
B. device and functional dependencies; and
C. third party libraries used.

If the application does not adhere to the requirements given above or the Consultant has unacceptable disclosures, at the State's discretion, the Consultant will rectify the issues at no cost to the State.

OFFSHORE SERVICES

The Consultant will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this Agreement without the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

MULTIFACTOR AUTHENTICATION

The Consultant's and the Consultant's subcontractors will not access the State's network except through the State's Multifactor Authentication process. For purposes of remote access to the State systems on the State's domain, the Consultant will adhere to the State's requirements for Multifactor Authentication upon receipt of notification from the State that such requirements have been implemented. The Consultant will also require adherence to the State's requirements by any of the Consultant's officers, employees, subcontractors, agents, assigns, and affiliated entities who will have remote access to State systems on the State's domain. The State's requirements for Multifactor Authentication are set forth in the State's Information Technology Security Policy, which is attached as Appendix.

CONSULTANT'S SOFTWARE LICENSES

The Consultant must disclose to the State the license(s) for any third-party software and libraries used by the Consultant's product(s) ((and/or) in the project by the Consultant) covered under this agreement if the State will not be the license(s) holder. The Consultant is required to provide copies of the license(s) for the third-party software and libraries to the State. No additional software and libraries may be added to the project after the contract is signed without notifying the State and providing the licenses of the software and libraries. Open source software and libraries are also covered by this clause. Any validation of any license(s) used by the Consultant to fulfil the Consultant's commitments agreed to in this agreement is the responsibility of the Consultant, not the State.

DATA SANITIZATION

At the end of the project covered by this Agreement the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88.

Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Consultant and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Consultant will use a process and procedure that does satisfy the State.

BANNED HARDWARE

The Consultant will not provide to the State any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huwaei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. The Consultant will immediately notify the State if the Consultant becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

USE OF PORTABLE DEVICES

The Consultant shall prohibit its employees, agents, affiliates and subcontractors form storing State data on portable devices, including personal computers, except for devices that are used and kept only at the Consultant's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

REMOTE ACCESS

The Consultant shall prohibit its employees, agents, affiliates and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

State of South Dakota

BIT Consultant Hosting, SaaS and Cloud Services State Technology Contract Template Terms

THIRD PARTY HOSTING

If the Consultant has the State's data hosted by another party the Consultant must provide the State, the name of this party. The Consultant must provide the State with contact information for this third party and the location of their data center(s). The Consultant must receive from the third party written assurances that the state's data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the consultant changes from the Consultant hosting the data to a third-party hosting the data or changes third-party hosting provider, the Consultant will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

SECURING OF DATA

All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

SECURITY PROCESSES

The Consultant shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Consultant. For example: virus checking and port sniffing.

IMPORT AND EXPORT OF DATA

The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Consultant. This includes the ability for the State to import or export data to/from other Consultants.

SCANNING AUTHORIZATION

The Consultant will provide the State at no cost and at a date, time and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security

scanning activities. The system and data provided to the State by Consultant for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. Consultant provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or that the consultant has with a third-party.

Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate, at the State's discretion with, the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Consultant. In the event of conflicting language this clause supersedes any other language in this, or any other agreement made between the State and the Consultant.

The Consultant agrees to work with the State to rectify any serious security issues revealed by security scanning. This includes additional security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Consultant and the State agree that scanning results cannot be achieved that are acceptable to the State, then the State may terminate the Agreement without further obligation.

SYSTEM UPGRADES

Advance notice of 30 days shall be provided the State of any major upgrades or system changes the Consultant will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Consultant's systems for vulnerabilities after a system upgrade. These vulnerability scan can include penetration testing of a test system at the State's discretion.

PASSWORD PROTECTION

The website(s) and or service(s) that will be hosted by the Consultant for the State will be password protected. If the Consultant provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Protected Health Information, Federal Tax Information or any information defined under state statute as Confidential Information or fragment thereof.

MOVEMENT OF PROTECTED STATE DATA

Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant's production or non-production systems, security must be maintained. The Consultant will ensure

that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP).

BANNED SERVICES

The Consultant warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS

If the Consultant is hosting on their system or performing Software as a Service where there is the potential for the Consultant and/or the Consultant's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Consultant's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

BIT Security and Vendor Questions

Security and Vendor Questions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. BIT recommends that you utilize your BIT Point of Contact to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards.

If you do not know the details of the technologies that vendors will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

Contractors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). You will see that these questions are divided into sections to help identify the point of the questions.

Use the last column as needed to explain your answers. Also note that many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been greyed out. **If the contractor answers a question by referencing another document or another part of the RFP response, they must give the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the branch that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact them on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contact

Section A: System Security

The following questions are relevant for all contractors or third parties engaged in this hardware, application or service and pertain to relevant security practices and procedures.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A1	DC	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on?				
A2	DC TELx	Will the system provide Internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?				
A3	POC	Will the system have role-based access?				

#	BIT	Question	Response YES	NO	NA	Explain answer as needed
A4	DC TEL	Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, Multi Factor authentication)? Which mitigations are in place? What are the optional mitigations?				
A5	DC TEL	Are account credentials hashed and encrypted when stored?				
A6	DC TEL x	The protection of the State's system and data is of upmost importance. Security scans must be done if: • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. **The State would want to scan a test system; not a production system and will not do penetration testing.** The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Are either of these an issue? If so, please explain.				
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?				
A8	POC x	Will organizations other than the State of South Dakota have access to our data?				
A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A10	DEV	Are there some requirements for security that are "structured" as part of general release readiness of a product, and others that are "as needed" or "custom" for a particular release?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
A13	TEL	What security criteria, if any, are considered when selecting third-party suppliers?				
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				
A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?				
A17	DC TEL x	Has the product undergone any vulnerability and/or penetration testing? If yes, how frequency, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?				
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				
A21	DC	What is your background check policy and procedure?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for				

		personnel working within the software development life cycle? Explain.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
A24	DC TEL	Do you have an automated Security Information and Event Management system?				
A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events				
		b. Application events				
		c. Authentication events				
		d. Physical access to your data center(s)				
		e. Code changes				
		f. Other				
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security-specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?				
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?				
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?				
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation/escalation?				
A31	DC TEL	Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?				

#	BIT	Question	Response YES	NO	NA	Explain answer as needed
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on implementing multifactor authentication? If so, when?				
A33	POC	Will this system provide the capability to track data entry/access by the person, date and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit done annually?				
		c. If it is SOC 2 audit report does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				
		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request, a redacted version is acceptable?				
A36		Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either				

		permanently or intermittently, are maintained and/or updated?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?				
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A39	DC	What are your policies and procedures for hardening servers?				
A40	DC TEL	(Only to be used when medical devices are being acquired.) Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date and the nature of the cybersecurity advisory.				
A41	DC POC	Does any product you propose to use or provide the State include software, hardware or hardware components manufactured by any company on the US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.				

Section B: Hosting

The following questions are relevant to any hosted applications, systems, databases, services, and any other technology. The responses should not assume a specific hosting platform, technology, or service but instead the response should address any hosting options available for the proposed solution.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?				
B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?				
B4	DC DEV POC TEL	Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster. Are warm or hot backups available? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?				
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?				
B7	DC DEV TEL	If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with: · Security for their I/T systems; · Staff vetting; · Staff security training?				
		a. If yes, summarize the contractual requirements.				
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?				
B8	DC	If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				

#	BIT	Question	Response YES	NO	NA	Explain answer as needed
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B10	DC	How do you secure Internet of Things (IoT) devices on your network?				
B11	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B12	DC TEL	Does your company have an endpoint detection and response policy?				
B13	DC TEL	Does your company have any real-time security auditing processes?				
B14	TEL	How do you perform analysis against the network traffic being transmitted or received by your application, systems and/or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B15	TEL	How do you monitor your application, systems and/or data center for security events, incidents or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	DC TEL	What anti-malware product(s) do you use?				
B17	DC TEL	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?				
B18	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
B19	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B20	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
B21	POC	Will the State of South Dakota own the data created in your hosting environment?				
B22	DEV	What are your record destruction scheduling capabilities?				

Section C: Database

Applies to any application or service that stores data, irrespective of the application being hosted by the state or the vendor.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explanation**
C1	DC	Will the system require a database?				
C2	DC	If a Database is required what technology will be used (i.e. Microsoft SQL Server, Oracle, MySQL)?				
C3	DC	If a SQL Database is required does the cost of the software include the cost of licensing the SQL Server?				
C4	POC	Will the system data be exportable by the user to tools like Excel or Access at all points during the workflow?				
C5	DC DEV	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?				
C6	DC DEV	Will the system infrastructure require a Business Intelligence solution?				

Section D: Contractor Process

The following questions are relevant for all contractors or third parties engaged in providing this hardware, application or service and pertain to business practices. If the application is hosted by the contractor or the contractor supplies cloud services those questions dealing with installation or support of applications on the State's system can be marked "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
D1	DC POC	Will the contractor provide assistance with installation?				
D2	DC DEV POC TEL	Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				
D5	TEL	What release criteria does your company have for its products regarding security?				

#	BIT		Question	Response YES	NO	NA	Explain answer as needed
D6	DEV		What controls are in place to ensure that only the accepted/released software is placed on media for distribution?				
D7	DCDEV	a.	b. Is there a Support Lifecycle Policy within the organization for the software in question?				
		c.	d. Does it outline and establish a consistent and predictable support timeline?				
D8	DC		How are patches, updates and service packs communicated and distributed to the State?				
D9	DEV		What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?				
D10	DC	a.	b. Can patches and Service Packs be uninstalled?				
		c.	d. Are the procedures for uninstalling a patch or Service Pack automated or manual?				
D11	DCDEV		How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized and reported? Is the management and reporting policy available for review?				
D12	DC		What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates and service packs?				
D13	DC		Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				

D 14	DEV		What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code or unintended, "dead," or malicious code? What tools are used?				
D 15	DEV		How is the software provenance verified (e.g. any checksums or signatures)?				
D 16	DEV	a.	b. Does the documentation explain how to install, configure, and/or use the software securely?				
		c.	d. Does it identify options that should not normally be used because they create security weaknesses?				
				Response			
#	**BIT**		**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
D 17	DEV	a.	b. Does your company develop security measurement objectives for all phases of the SDLC?				
		c.	d. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D 18	DC	a.	b. Is testing done after changes are made to servers?				
		c.	d. What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?				
D 19	DC		What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?				

D20	DCTEL		How is endpoint protection done for example is virus prevention used, and how are detection, correction, and updates handled?				
D21	DCTEL		Do you perform regular reviews of system and network logs for security issues?				
D22	DC		Do you provide security performance measures to the customer at regular intervals?				
D23	DCPOC		What technical, installation and user documentation, do you provide to the State? Is the documentation electronically available and can it be printed?				
D24	DCDEVPOC	a.	b. Will the implementation plan include user acceptance testing?				
		c.	d. If yes what were the test cases?				
		e.	f. Do you do software assurance?				
D25	DCDEVPOCTEL		Will the implementation plan include performance testing?				
D26	DEVPOC		Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEVPOC		If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEVPOC		Has your company ever conducted a project where your product was load tested?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization and processes that created the software.				
D30	DC	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.				
D31	TEL DC DEV	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation.				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software.				
D33	DC DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?				
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?				
D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of “trigger” events.				

D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
D38	DC DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. Include training specifically given to your developers on secure development.				
D39	DC TEL x	It is State policy that all Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?				
D40	POC TEL x	Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State's discretion, a contractor's answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(For PHI only) a. Have you done a risk assessment? If yes, will you share it?				
		b. If you have not done a risk assessment, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development						
The following questions pertain to the tools and third-party components used to develop your application, irrespective of the application being hosted by the State or the vendor						
			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
E1	DEV POC x	What are the development technologies used for this system? Please indicate version as appropriate				
		ASP.Net				
		VB.Net				
		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based User Interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to				

		exchange data between diverse computing platforms?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
E12	DC	a. If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)?				
		b. If so, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	Does the exception handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				
		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?				
		c. Do you have support agreements for these applications?				
E20	DC	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.				
E21	TEL	a. Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)?				

		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device what is your process for making sure your application can run on the newest version of the mobile device's operating system?				
E24	DEV	Do you use open source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				

Section F: Infrastructure

This pertains to how your system interacts with the State's technology infrastructure. If the proposed technology does not interact with the State's system, the questions can be marked as "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
F1	TEL	Is there a workstation install requirement?				
F2	DC	Will the system infrastructure have a special backup requirement?				
F3	DC	Will the system infrastructure have any processes that require scheduling?				
F4	DC	The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?				
F5	TEL x	Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?				
F6	DC x	It is State policy that all systems must be compatible with BIT's dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?				
F7	TEL x	It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.				
F8	DC	It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F9	DC x	The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.				
F10	TEL x	It is State policy that all access from outside of the State of South Dakota's private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this				

		affect the implementation of the system? If yes, explain.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F11	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F12	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.				
F13	DC	The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?				
F14	POC TEL	Please describe the types and levels of network access your system/application will require. This should include, but not be limited to TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F15	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				
F16	DC	Will your application require a dedicated environment?				
F17	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				

F18	DC TEL	Provide a system diagram to include the components of the system, description of the component and how the components communicate with each other.				

			Response			
#	BIT	Question	YES	NO	NA	Explain answer as needed
F19	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F20	TEL x	It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?				
F21	DC x	Will the server-based software support: a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard Edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
		h. Symantec End Point Protection				
F22	TEL x	All network systems must operate within the current configurations of the State of South Dakota's firewalls, switches, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?				
F23	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F24	DC TEL	The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll outs of any and all Microsoft patches based on level of criticality. Do you have any concerns regarding this process?				
F25	DC TEL	What physical access do you require to work on hardware?				
F26	DC	How many of the Vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process

These questions relate to how your business model interacts with the State's policies, procedures and practices. If the vendor is hosting the application or providing cloud services questions dealing with installation or support of applications on the State's system the questions can be marked "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
G1	DC	a. If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?				
		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	POC	Explain the software licensing model.				
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?				
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?				
		b. If yes, are there any additional costs for the customization?				
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.				
G6	POC	Contractually, how many years price lock will you offer the State as part of your response? Also, as part of your response, how many additional years are you offering to limit price increases and by what percent?				
G7	POC	Will the State acquire the data at contract conclusion?				
G8	POC	Will the State's data be used for any other purposes other than South Dakota's usage?				
G9	DC	Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.				
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G11	DC	Please summarize your company's history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).				

#	BIT	Question	Response			
			YES	NO	NA	Explain answer as needed
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?				
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?				
G15	DC	Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk and transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?				
G18	DC POCx	Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				

BIT Scanning Permission Form

The vendor acknowledges that the State will be able to do a security scan of the vendor's product or service. This will be a vulnerability scan that will not include a penetration test. The State will use industry standard tools. The State prefers to scan a non-production environment with non-production data. These scans will be done at mutually agreeable times. At the option of the State, a scan that demonstrates that the vendor's product or service meets the State's security requirements can be done either before an agreement between the State and the vendor is signed or after. The vendor should fill in the information below and sign this form authorizing the State to do a security scan. The vendor's employee signing this form must have the authority to commit the vendor to allowing the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. Any RFP response that does not include this signed form will be considered incomplete and may be excluded from further consideration.

Vendor's name: _____

Vendor's security contact's name: _____

Security contact's phone number: _____

Security contact's email address: _____

Web address URL or product name _____ The State will contact the security contact listed above to arrange for a test log in for the scanning.

Vendor's employee acknowledging the right to scan (Print):_____

Title: _____

Date: _____

Signature: _____

BIT Security Acknowledgement

Please return agreement to your BIT Manager or Designated BIT Contact

All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy").** Users are responsible for compliance to all information security policies and procedures. *By signature below, the employee or contractor hereby acknowledges and agrees to the following:*

1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;
2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Employee or contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;
4. Employee or contractor has read and agrees to abide by the Policy;
5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;
6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;
7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;
10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.

Information Technology Security Policy – BIT: http://intranet.bit.sd.gov/policies/
Information Technology Security Policy – CLIENT: http://intranet.bit.sd.gov/policies/
Information Technology Security Policy – CONTRACTOR: http://bit.sd.gov/vendor/default.aspx

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

_____ _____ _____ _____
Employee or Contractor signature Date BIT Manager or Contact Date

_____
Employee or Contractor name and Company name in block capital letters

Federal Certification and Clauses

ACCESS TO RECORDS AND REPORTS

a. Record Retention. The Contractor will retain, and will require its subcontractors of all tiers to retain, complete and readily accessible records related in whole or in part to the contract, including, but not limited to, data, documents, reports, statistics, sub-Contracts, leases, subcontracts, arrangements, other third party Contracts of any type, and supporting materials related to those records.

b. Retention Period. The Contractor agrees to comply with the record retention requirements in accordance with 2 C.F.R. § 200.333. The Contractor shall maintain all books, records, accounts and reports required under this Contract for a period of at not less than three (3) years after the date of termination or expiration of this Contract, except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case records shall be maintained until the disposition of all such litigation, appeals, claims or exceptions related thereto.

c. Access to Records. The Contractor agrees to provide sufficient access to FTA and its contractors to inspect and audit records and information related to performance of this contract as reasonably may be required.

d. Access to the Sites of Performance. The Contractor agrees to permit FTA and its contractors access to the sites of performance under this contract as reasonably may be required.

AMERICANS WITH DISABILITIES ACT(ADA)

The contractor agrees to comply with the requirements of 49 U.S.C. § 5301 (d), which states the Federal policy that the elderly and persons with disabilities have the same right as other persons to use mass transportation service and facilities, and that special efforts shall be made in planning and designing those services and facilities to implement that policy. The contractor also agrees to comply with all applicable requirements of section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794, which prohibits discrimination on the basis of handicaps, with the Americans with Disabilities Act of 1990 (ADA), as amended, 42 U.S.C. §§ 12101 et seq., which requires that accessible facilities and services be made available to persons with disabilities, including any subsequent amendments to that Act, and with the Architectural Barriers act of 1968, as amended, 42 U.S.C. §§ 4151 et seq., which requires that buildings and public accommodations be accessible to persons with disabilities, including any subsequent amendments to that Act. In addition, the contractor agrees to comply with any and all applicable requirements issued by the FTA, DOT, DOJ, U.S. GSA, U.S. EEOC, U.S. FCC, any subsequent amendments thereto and any other nondiscrimination statute(s) that may apply to the Project.

BUY AMERICA REQUIREMENTS

The contractor agrees to comply with 49 U.S.C. 5323(j) and 49 C.F.R. part 661 and 2 CFR § 200.322 Domestic preferences for procurements, which provide that Federal funds may not be obligated unless all steel, iron, and manufactured products used in FTA funded projects are

produced in the United States, unless a waiver has been granted by FTA or the product is subject to a general waiver. General waivers are listed in 49 C.F.R. § 661.7. Separate requirements for rolling stock are set out at 49 U.S.C. 5323(j)(2)(C), 49 U.S.C. § 5323(u) and 49 C.F.R. § 661.11. The bidder or vendor must submit to the Agency the appropriate Buy America certification. Bids or offers that are not accompanied by a completed Buy America certification will be rejected as nonresponsive.

BYRD ANTI-LOBBYING AMENDMENT

Contractors who apply or bid for an award of $100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the Agency."

CARGO PREFERENCE REQUIREMENTS

The contractor agrees:
a. to use privately owned United States-Flag commercial vessels to ship at least 50 percent of the gross tonnage (computed separately for dry bulk carriers, dry cargo liners, and tankers) involved, whenever shipping any equipment, material, or commodities pursuant to the underlying contract to the extent such vessels are available at fair and reasonable rates for United States-Flag commercial vessels;

b. to furnish within 20 working days following the date of loading for shipments originating within the United States or within 30 working days following the date of loading for shipments originating outside the United States, a legible copy of a rated, "on-board" commercial ocean bill-of-lading in English for each shipment of cargo described in the preceding paragraph to the Division of National Cargo, Office of Market Development, Maritime Administration, Washington, DC 20590 and to the FTA Recipient (through the contractor in the case of a subcontractor's bill-of-lading.); and

c. to include these requirements in all subcontracts issued pursuant to this contract when the subcontract may involve the transport of equipment, material, or commodities by ocean vessel.

CIVIL RIGHTS LAWS AND REGULATIONS

The following Federal Civil Rights laws and regulations apply to all contracts.

1 Federal Equal Employment Opportunity (EEO) Requirements. These include, but are not limited to:

a) Nondiscrimination in Federal Public Transportation Programs. 49 U.S.C. § 5332, covering projects, programs, and activities financed under 49 U.S.C. Chapter 53, prohibits discrimination on the basis of race, color, religion, national origin, sex (including sexual orientation and gender identity), disability, or age, and prohibits discrimination in employment or business opportunity.

b) Prohibition against Employment Discrimination. Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e, and Executive Order No. 11246, “Equal Employment Opportunity,” September 24, 1965, as amended, prohibit discrimination in employment on the basis of race, color, religion, sex, or national origin.

2 Nondiscrimination on the Basis of Sex. Title IX of the Education Amendments of 1972, as amended, 20 U.S.C. § 1681 et seq. and implementing Federal regulations, “Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance,” 49 C.F.R. part 25 prohibit discrimination on the basis of sex.

3 Nondiscrimination on the Basis of Age. The “Age Discrimination Act of 1975,” as amended, 42 U.S.C. § 6101 et seq., and Department of Health and Human Services implementing regulations, “Nondiscrimination on the Basis of Age in Programs or Activities Receiving Federal Financial Assistance,” 45 C.F.R. part 90, prohibit discrimination by participants in federally assisted programs against individuals on the basis of age. The Age Discrimination in Employment Act (ADEA), 29 U.S.C. § 621 et seq., and Equal Employment Opportunity Commission (EEOC) implementing regulations, “Age Discrimination in Employment Act,” 29 C.F.R. part 1625, also prohibit employment discrimination against individuals age 40 and over on the basis of age.

4 Federal Protections for Individuals with Disabilities. The Americans with Disabilities Act of 1990, as amended (ADA), 42 U.S.C. § 12101 et seq., prohibits discrimination against qualified individuals with disabilities in programs, activities, and services, and imposes specific requirements on public and private entities. Third party contractors must comply with their responsibilities under Titles I, II, III, IV, and V of the ADA in employment, public services, public accommodations, telecommunications, and other provisions, many of which are subject to regulations issued by other Federal agencies.

Civil Rights and Equal Opportunity
The Agency is an Equal Opportunity Employer. As such, the Agency agrees to comply with all applicable Federal civil rights laws and implementing regulations. Apart from inconsistent requirements imposed by Federal laws or regulations, the Agency agrees to comply with the requirements of 49 U.S.C. § 5323(h) (3) by not using any Federal assistance awarded by FTA to support procurements using exclusionary or discriminatory specifications. Under this Contract, the Contractor shall at all times comply with the following requirements and shall include these requirements in each subcontract entered into as part thereof.

1. Nondiscrimination. In accordance with Federal transit law at 49 U.S.C. § 5332, the Contractor agrees that it will not discriminate against any employee or applicant for employment because of race, color, religion, national origin, sex, disability, or age. In addition, the Contractor agrees to comply with applicable Federal implementing regulations and other implementing requirements FTA may issue.

2. Race, Color, Religion, National Origin, Sex. In accordance with Title VII of the Civil Rights Act, as amended, 42 U.S.C. § 2000e et seq., and Federal transit laws at 49 U.S.C. § 5332, the Contractor agrees to comply with all applicable equal employment opportunity requirements of U.S. Department of Labor (U.S. DOL) regulations, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," 41 C.F.R. chapter 60, and Executive Order No. 11246, "Equal Employment Opportunity in Federal Employment," September 24, 1965, 42 U.S.C. § 2000e note, as amended by any later Executive Order that

amends or supersedes it, referenced in 42 U.S.C. § 2000e note. The Contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, national origin, or sex (including sexual orientation and gender identity). Such action shall include, but not be limited to, the following: employment, promotion, demotion or transfer, recruitment or recruitment advertising, layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. In addition, the Contractor agrees to comply with any implementing requirements FTA may issue.

3. Age. In accordance with the Age Discrimination in Employment Act, 29 U.S.C. §§ 621-634, U.S. Equal Employment Opportunity Commission (U.S. EEOC) regulations, "Age Discrimination in Employment Act," 29 C.F.R. part 1625, the Age Discrimination Act of 1975, as amended, 42 U.S.C. § 6101 et seq., U.S. Health and Human Services regulations, "Nondiscrimination on the Basis of Age in Programs or Activities Receiving Federal Financial Assistance," 45 C.F.R. part 90, and Federal transit law at 49 U.S.C. § 5332, the Contractor agrees to refrain from discrimination against present and prospective employees for reason of age. In addition, the Contractor agrees to comply with any Implementing requirements FTA may issue.

4.Disabilities. In accordance with section 504 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794, the Americans with Disabilities Act of 1990, as amended, 42 U.S.C. § 12101 et seq., the Architectural Barriers Act of 1968, as amended, 42 U.S.C. § 4151 et seq., and Federal transit law at 49 U.S.C. § 5332, the Contractor agrees that it will not discriminate against individuals on the basis of disability. In addition, the Contractor agrees to comply with any implementing requirements FTA may issue.

5.Promoting Free Speech and Religious Liberty. The Contractor shall ensure that Federal funding is expended in full accordance with the U.S. Constitution, Federal Law, and statutory and public policy requirements: including, but not limited to, those protecting free speech, religious liberty, public welfare, the environment, and prohibiting discrimination.

CLEAN AIR ACT AND FEDERAL WATER POLLUTION CONTROL ACT

The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. § 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. § 1251-1387). Violations must be reported to FTA and the Regional Office of the Environmental Protection Agency. The following applies for contracts of amounts in excess of $150,000:

Clean Air Act

(1) The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

(2) The contractor agrees to report each violation to the Agency and understands and agrees that the Agency will, in turn, report each violation as required to assure notification to the Agency, Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

(3) The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FTA.

Federal Water Pollution Control Act

(1) The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

(2) The contractor agrees to report each violation to the Agency and understands and agrees that the Agency will, in turn, report each violation as required to assure notification to the Agency, Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

(3) The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FTA."

CONFORMANCE WITH ITS NATIONAL ARCHITECTURE

Intelligent Transportation Systems (ITS) projects shall conform to the National ITS Architecture and standards. Conformance with the National ITS Architecture is interpreted to mean the use of the National ITS Architecture to develop a regional ITS architecture in support of integration and the subsequent adherence of all ITS projects to that regional ITS architecture. Development of the regional ITS architecture should be consistent with the transportation planning process for Statewide and Metropolitan Transportation Planning (49 CFR Part 613 and 621).

DEBARMENT AND SUSPENSION

a. Applicability: This requirement applies to all FTA grant and cooperative agreement programs for a contract in the amount of at least $25,000

(1) This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such the contractor is required to verify that none of the contractor, its principals (defined at 2 C.F.R. § 180.995), or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(2) C.F.R. pt. 3000, subpart C and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(3) The accompanying certification is a material representation of fact relied upon by the subrecipient. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the Agency and subrecipient, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions."

DISADVANTAGED BUSINESS ENTERPRISE (DBE)

The contractor or subcontractor shall not discriminate on the basis of race, color, national origin, or sex in the performance of this contract. The contractor shall carry out applicable requirements of 49 C.F.R. part 26 in the award and administration of DOT-assisted contracts. Failure by the contractor to carry out these requirements is a material breach of this contract, which may result in the termination of this contract or such other remedy as the Agency deems appropriate, which may include, but is not limited to:

(1) Withholding monthly progress payments; (2) Assessing sanctions; (3) Liquidated damages; and/or (4) Disqualifying the contractor from future bidding as non-responsible. 49 C.F.R. § 26.13(b).

Prime contractors are required to pay subcontractors for satisfactory performance of their contracts no later than 30 days from receipt of each payment the Agency makes to the prime contractor. 49 C.F.R. § 26.29(a).

Finally, for contracts with defined DBE contract goals, each FTA Recipient must include in each prime contract a provision stating that the contractor shall utilize the specific DBEs listed unless the contractor obtains the Agency's written consent; and that, unless the Agency's consent is provided, the contractor shall not be entitled to any payment for work or material unless it is performed or supplied by the listed DBE. 49 C.F.R. § 26.53(f) (1).

It is the policy of the Agency and the United States Department of Transportation ("DOT") that Disadvantaged Business Enterprises ("DBE's"), as defined herein and in the Federal regulations published at 49 C.F.R. part 26, shall have an equal opportunity to participate in DOT-assisted contracts.

DHS SEAL, LOGO, AND FLAGS

The contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FTA pre-approval.

ENERGY CONSERVATION

The contractor agrees to comply with mandatory standards and policies relating to energy efficiency, which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act.

EQUAL EMPLOYMENT OPPORTUNITY

During the performance of this contract, the contractor agrees as follows:

(1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the

following: Employment, upgrading, demotion, or transfer, recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

(2) The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

(4) The contractor will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under section 202 of Executive Order 11246 of September 24, 1965, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by the rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the contracting agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the contractor's non-compliance with the nondiscrimination clauses of this contract or with any of such rules, regulations, or orders, this contract may be canceled, terminated or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The contractor will include the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as may be directed by the Secretary of

Labor as a means of enforcing such provisions including sanctions for noncompliance: Provided, however, that in the event the contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

FEDERAL CHANGES

49 CFR Part 18 Federal Changes - Contractor shall at all times comply with all applicable FTA regulations, policies, procedures and directives, including without limitation those listed directly or by reference in the Master Agreement between Purchaser and FTA, as they may be amended or promulgated from time to time during the term of this contract. Contractor's failure to so comply shall constitute a material breach of this contract.

FLY AMERICA

a) Definitions. As used in this clause—
1) “International air transportation” means transportation by air between a place in the United States and a place outside the United States or between two places both of which are outside the United States. 2) “United States” means the 50 States, the District of Columbia, and outlying areas. 3) “U.S.-flag air carrier” means an air carrier holding a certificate under 49 U.S.C. Chapter 411.

b) When Federal funds are used to fund travel, Section 5 of the International Air Transportation Fair Competitive Practices Act of 1974 (49 U.S.C. 40118) (Fly America Act) requires contractors, Agencys, and others use U.S.-flag air carriers for U.S. Government-financed international air transportation of personnel (and their personal effects) or property, to the extent that service by those carriers is available. It requires the Comptroller General of the United States, in the absence of satisfactory proof of the necessity for foreign-flag air transportation, to disallow expenditures from funds, appropriated or otherwise established for the account of the United States, for international air transportation secured aboard a foreign-flag air carrier if a U.S.-flag air carrier is available to provide such services.

c) If available, the Contractor, in performing work under this contract, shall use U.S.-flag carriers for international air transportation of personnel (and their personal effects) or property.

d) In the event that the Contractor selects a carrier other than a U.S.-flag air carrier for international air transportation, the Contractor shall include a statement on vouchers involving such transportation essentially as follows:

Statement of Unavailability of U.S.-Flag Air Carriers
International air transportation of persons (and their personal effects) or property by U.S.-flag air carrier was not available or it was necessary to use foreign-flag air carrier service for the following reasons. See FAR § 47.403. [State reasons]:

e) Contractor shall include the substance of this clause, including this paragraph (e), in each subcontract or purchase under this contract that may involve international air transportation.

INCORPORATION OF FEDERAL TRANSIT ADMINISTRATION (FTA) TERMS

Incorporation of Federal Transit Administration (FTA) Terms - The provisions within include, in part, certain Standard Terms and Conditions required by DOT, whether or not expressly set forth in the preceding contract provisions. All contractual provisions required by DOT, as set forth in the current FTA Circular 4220 are hereby incorporated by reference. Anything to the contrary herein notwithstanding, all FTA mandated terms shall be deemed to control in the event of a conflict with other provisions contained in this Contract. The Contractor shall not perform any act, fail to perform any act, or refuse to comply with any request which would cause a violation of the FTA terms and conditions.

NO GOVERNMENT OBLIGATION TO THIRD PARTIES

The Agency and Contractor acknowledge and agree that, notwithstanding any concurrence by the Federal Government in or approval of the solicitation or award of the underlying Contract, absent the express written consent by the Federal Government, the Federal Government is not a party to this Contract and shall not be subject to any obligations or liabilities to the Agency, Contractor or any other party (whether or not a party to that contract) pertaining to any matter resulting from the underlying Contract. The Contractor agrees to include the above clause in each subcontract financed in whole or in part with Federal assistance provided by the FTA. It is further agreed that the clause shall not be modified, except to identify the subcontractor who will be subject to its provisions.

NOTIFICATION TO FTA

If a current or prospective legal matter that may affect the Federal Government emerges, the Recipient must promptly notify the FTA Chief Counsel and FTA Regional Counsel for the Region in which the Recipient is located. The Recipient must include a similar notification requirement in its Third Party Agreements and must require each Third Party Participant to include an equivalent provision in its sub agreements at every tier, for any agreement that is a “covered transaction” according to 2 C.F.R. §§ 180.220 and 1200.220.

(1) The types of legal matters that require notification include, but are not limited to, a major dispute, breach, default, litigation, or naming the Federal Government as a party to litigation or a legal disagreement in any forum for any reason.

(2) Matters that may affect the Federal Government include, but are not limited to, the Federal Government’s interests in the Award, the accompanying Underlying Agreement, and any Amendments thereto, or the Federal Government’s administration or enforcement of federal laws, regulations, and requirements.

(3) The Recipient must promptly notify the U.S. DOT Inspector General in addition to the FTA Chief Counsel or Regional Counsel for the Region in which the Recipient is located, if the Recipient has knowledge of potential fraud, waste, or abuse occurring on a Project receiving assistance from FTA. The notification provision applies if a person has or may have submitted a false claim under the False Claims Act, 31 U.S.C. § 3729 et seq., or has or may have committed a criminal or civil violation of law pertaining to such matters as fraud, conflict of interest, bribery, gratuity, or similar misconduct. This responsibility occurs whether the Project is subject to this Agreement or another agreement between the Recipient and FTA, or an agreement involving a principal, officer, employee, agent, or Third Party Participant of the Recipient. It also applies to subcontractors at any tier. Knowledge, as used in this paragraph, includes, but is not limited to,

knowledge of a criminal or civil investigation by a Federal, state, or local law enforcement or other investigative agency, a criminal indictment or civil complaint, or probable cause that could support a criminal indictment, or any other credible information in the possession of the Recipient.

PROCUREMENT OF RECOVERED MATERIALS

(1) In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA- designated items unless the product cannot be acquired—
i. Competitively within a timeframe providing for compliance with the contract performance schedule;
ii. Meeting contract performance requirements; or
iii. At a reasonable price.

(2) Information about this requirement, along with the list of EPA-designate items, is available at EPA's Comprehensive Procurement Guidelines web site,
https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program."

PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS AND RELATED ACTS

The contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the contractor's actions pertaining to this contract."

PROMPT PAYMENT

The contractor is required to pay its subcontractors performing work related to this contract for satisfactory performance of that work no later than 30 days after the contractor's receipt of payment for that work. In addition, the contractor is required to return any retainage payments to those subcontractors within 30 days after the subcontractor's work related to this contract is satisfactorily completed.

The contractor must promptly notify the Agency, whenever a DBE subcontractor performing work related to this contract is terminated or fails to complete its work and must make good faith efforts to engage another DBE subcontractor to perform at least the same amount of work. The contractor may not terminate any DBE subcontractor and perform that work through its own forces or those of an affiliate without prior written consent of the Agency.

SAFE OPERATION OF MOTOR VEHICLES

Seat Belt Use
The Contractor is encouraged to adopt and promote on-the-job seat belt use policies and programs for its employees and other personnel that operate company-owned vehicles, company rented vehicles, or personally operated vehicles. The terms "company-owned" and "company-leased" refer to vehicles owned or leased either by the Contractor or Agency.

Distracted Driving
The Contractor agrees to adopt and enforce workplace safety policies to decrease crashes caused by distracted drivers, including policies to ban text messaging while using an electronic device supplied by an employer, and driving a vehicle the driver owns or rents, a vehicle Contactor owns, leases, or rents, or a privately-owned vehicle when on official business in connection with the work performed under this Contract.

SPECIAL NOTIFICATION REQUIREMENTS FOR STATES

Applies to States –

a. To the extent required under federal law, the State, as the Recipient, agrees to provide the following information about federal assistance awarded for its State Program, Project, or related activities:

(1) The Identification of FTA as the federal agency providing the federal assistance for a State Program or Project;
(2) The Catalog of Federal Domestic Assistance Number of the program from which the federal assistance for a State Program or Project is authorized; and
(3) The amount of federal assistance FTA has provided for a State Program or Project.

b. Documents - The State agrees to provide the information required under this provision in the following documents: (1) applications for federal assistance, (2) requests for proposals or solicitations, (3) forms, (4) notifications, (5) press releases, and (6) other publications.

SIMPLIFIED ACQUISITION THRESHOLD

Contracts for more than the simplified acquisition threshold, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. § 1908, or otherwise set by law, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate. (Note that the simplified acquisition threshold determines the procurement procedures that must be employed pursuant to 2 C.F.R. §§ 200.317–200.327. The simplified acquisition threshold does not exempt a procurement from other eligibility or processes requirements that may apply. For example, Buy America's eligibility and process requirements apply to any procurement in excess of $150,000. 49 U.S.C. § 5323(j)(13).

TERMINATION

Termination for Convenience (General Provision)
The Agency may terminate this contract, in whole or in part, at any time by written notice to the Contractor when it is in the Agency's best interest. The Contractor shall be paid its costs, including contract close-out costs, and profit on work performed up to the time of termination. The Contractor shall promptly submit its termination claim to Agency to be paid the Contractor. If the Contractor has any property in its possession belonging to Agency, the Contractor will account for the same, and dispose of it in the manner Agency directs.

Termination for Default [Breach or Cause] (General Provision)
If the Contractor does not deliver supplies in accordance with the contract delivery schedule, or if the contract is for services, the Contractor fails to perform in the manner called for in the contract, or if the Contractor fails to comply with any other provisions of the contract, the Agency may terminate this contract for default. Termination shall be effected by serving a Notice of Termination on the Contractor setting forth the manner in which the Contractor is in default. The Contractor will be paid only the contract price for supplies delivered and accepted, or services performed in accordance with the manner of performance set forth in the contract. If it is later determined by the Agency that the Contractor had an excusable reason for not performing, such as a strike, fire, or flood, events which are not the fault of or are beyond the control of the Contractor, the Agency, after setting up a new delivery of performance schedule, may allow the Contractor to continue work, or treat the termination as a Termination for Convenience.

Opportunity to Cure (General Provision)
The Agency, in its sole discretion may, in the case of a termination for breach or default, allow the Contractor [an appropriately short period of time] in which to cure the defect. In such case, the Notice of Termination will state the time period in which cure is permitted and other appropriate conditions

If Contractor fails to remedy to Agency's satisfaction the breach or default of any of the terms, covenants, or conditions of this Contract within [10 days] after receipt by Contractor of written notice from Agency setting forth the nature of said breach or default, Agency shall have the right to terminate the contract without any further obligation to Contractor. Any such termination for default shall not in any way operate to preclude Agency from also pursuing all available remedies against Contractor and its sureties for said breach or default.

Waiver of Remedies for any Breach
In the event that Agency elects to waive its remedies for any breach by Contractor of any covenant, term or condition of this contract, such waiver by Agency shall not limit Agency’s remedies for any succeeding breach of that or of any other covenant, term, or condition of this contract.

Termination for Convenience (Professional or Transit Service Contracts)
The Agency, by written notice, may terminate this contract, in whole or in part, when it is in the Agency’s interest. If this contract is terminated, the Agency shall be liable only for payment under the payment provisions of this contract for services rendered before the effective date of termination.

Termination for Default (Supplies and Service)
If the Contractor fails to deliver supplies or to perform the services within the time specified in this contract or any extension, or if the Contractor fails to comply with any other provisions of this contract, the Agency may terminate this contract for default. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature of the default. The Contractor will only be paid the contract price for supplies delivered and accepted, or services performed in accordance with the manner or performance set forth in this contract. If, after termination for failure to fulfill contract obligations, it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Agency.

Termination for Default (Transportation Services)
If the Contractor fails to pick up the commodities or to perform the services, including delivery services, within the time specified in this contract or any extension, or if the Contractor fails to comply with any other provisions of this contract, the Agency may terminate this contract for default. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature of default. The Contractor will only be paid the contract price for services performed in accordance with the manner of performance set forth in this contract.

If this contract is terminated while the Contractor has possession of Agency goods, the Contractor shall, upon direction of the Agency, protect and preserve the goods until surrendered to the Agency or its agent. The Contractor and Agency shall agree on payment for the preservation and protection of goods. Failure to agree on an amount will be resolved under the Dispute clause.

If, after termination for failure to fulfill contract obligations, it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Agency.

Termination for Default (Construction)
If the Contractor refuses or fails to prosecute the work or any separable part, with the diligence that will ensure its completion within the time specified in this contract or any extension or fails to complete the work within this time, or if the Contractor fails to comply with any other provision of this contract, Agency may terminate this contract for default. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature of the default. In this event, the Agency may take over the work and compete it by contract or otherwise, and may take possession of and use any materials, appliances, and plant on the work site necessary for completing the work. The Contractor and its sureties shall be liable for any damage to the Agency resulting from the Contractor's refusal or failure to complete the work within specified time, whether or not the Contractor's right to proceed with the work is terminated. This liability includes any increased costs incurred by the Agency in completing the work.

The Contractor's right to proceed shall not be terminated nor shall the Contractor be charged with damages under this clause if: 1. The delay in completing the work arises from unforeseeable causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include: acts of God, acts of Agency, acts of another contractor in the performance of a contract with Agency, epidemics, quarantine restrictions, strikes, freight embargoes; and 2. The Contractor, within [10] days from the beginning of any delay, notifies Agency in writing of the causes of delay. If, in the judgment of Agency, the delay is excusable, the time for completing the work shall be extended. The judgment of Agency shall be final and conclusive for the parties, but subject to appeal under the Disputes clause(s) of this contract. 3. If, after termination of the Contractor's right to proceed, it is determined that the Contractor was not in default, or that the delay was excusable, the rights and obligations of the parties will be the same as if the termination had been issued for the convenience of Agency.

Termination for Convenience or Default (Architect and Engineering)
The Agency may terminate this contract in whole or in part, for the Agency’s convenience or because of the failure of the Contractor to fulfill the contract obligations. The Agency shall terminate by delivering to the Contractor a Notice of Termination specifying the nature, extent, and effective date of the termination. Upon receipt of the notice, the Contractor shall (1) immediately discontinue all services affected (unless the notice directs otherwise), and (2) deliver

to the Agency ‘s Contracting Officer all data, drawings, specifications, reports, estimates, summaries, and other information and materials accumulated in performing this contract, whether completed or in process. Agency has a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, all such data, drawings, specifications, reports, estimates, summaries, and other information and materials.

If the termination is for the convenience of the Agency, the Agency’s Contracting Officer shall make an equitable adjustment in the contract price but shall allow no anticipated profit on unperformed services. If the termination is for failure of the Contractor to fulfill the contract obligations, the Agency may complete the work by contact or otherwise and the Contractor shall be liable for any additional cost incurred by the Agency. If, after termination for failure to fulfill contract obligations, it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of Agency

Termination for Convenience or Default (Cost-Type Contracts)
The Agency may terminate this contract, or any portion of it, by serving a Notice of Termination on the Contractor. The notice shall state whether the termination is for convenience of Agency or for the default of the Contractor. If the termination is for default, the notice shall state the manner in which the Contractor has failed to perform the requirements of the contract. The Contractor shall account for any property in its possession paid for from funds received from the Agency, or property supplied to the Contractor by the Agency. If the termination is for default, the Agency may fix the fee, if the contract provides for a fee, to be paid the Contractor in proportion to the value, if any, of work performed up to the time of termination. The Contractor shall promptly submit its termination claim to the Agency and the parties shall negotiate the termination settlement to be paid the Contractor.

If the termination is for the convenience of Agency, the Contractor shall be paid its contract close-out costs, and a fee, if the contract provided for payment of a fee, in proportion to the work performed up to the time of termination.

If, after serving a Notice of Termination for Default, the Agency determines that the Contractor has an excusable reason for not performing, the Agency, after setting up a new work schedule, may allow the Contractor to continue work, or treat the termination as a Termination for Convenience.

VIOLATION AND BREACH OF CONTRACT

Rights and Remedies of the Agency
The Agency shall have the following rights in the event that the Agency deems the Contractor guilty of a breach of any term under the Contract.

1. The right to take over and complete the work or any part thereof as agency for and at the expense of the Contractor, either directly or through other contractors; 2. The right to cancel this Contract as to any or all of the work yet to be performed; 3. The right to specific performance, an injunction or any other appropriate equitable remedy; and 4. The right to money damages.

For purposes of this Contract, breach shall include.

Rights and Remedies of Contractor
Inasmuch as the Contractor can be adequately compensated by money damages for any breach of this Contract, which may be committed by the Agency, the Contractor expressly agrees that no default, act or omission of the Agency shall constitute a material breach of this Contract, entitling Contractor to cancel or rescind the Contract (unless the Agency directs Contractor to do so) or to suspend or abandon performance.

Remedies
Substantial failure of the Contractor to complete the Project in accordance with the terms of this Contract will be a default of this Contract. In the event of a default, the Agency will have all remedies in law and equity, including the right to specific performance, without further assistance, and the rights to termination or suspension as provided herein. The Contractor recognizes that in the event of a breach of this Contract by the Contractor before the Agency takes action contemplated herein, the Agency will provide the Contractor with sixty (60) days written notice that the Agency considers that such a breach has occurred and will provide the Contractor a reasonable period of time to respond and to take necessary corrective action.

Disputes
Disputes arising in the performance of this Contract that are not resolved by agreement of the parties shall be decided in writing by an authorized representative of Agency. This decision shall be final and conclusive unless within [10] days from the date of receipt of its copy, the Contractor mails or otherwise furnishes a written appeal to the Agency's authorized representative. In connection with any such appeal, the Contractor shall be afforded an opportunity to be heard and to offer evidence in support of its position. The decision of the Agency's authorized representative shall be binding upon the Contractor and the Contractor shall abide be the decision.

In the event that a resolution of the dispute is not mutually agreed upon, the parties can agree to mediate the dispute or proceed with litigation. Notwithstanding any provision of this section, or any other provision of this Contract, it is expressly agreed and understood that any court proceeding arising out of a dispute under the Contract shall be heard by a Court de novo and the court shall not be limited in such proceeding to the issue of whether the Authority acted in an arbitrary, capricious or grossly erroneous manner.

Pending final settlement of any dispute, the parties shall proceed diligently with the performance of the Contract, and in accordance with the Agency's direction or decisions made thereof.

Performance during Dispute
Unless otherwise directed by Agency, Contractor shall continue performance under this Contract while matters in dispute are being resolved.

Claims for Damages
Should either party to the Contract suffer injury or damage to person or property because of any act or omission of the party or of any of its employees, agents or others for whose acts it is legally liable, a claim for damages therefor shall be made in writing to such other party within a reasonable time after the first observance of such injury or damage.

Remedies
Unless this Contract provides otherwise, all claims, counterclaims, disputes and other matters in question between the Agency and the Contractor arising out of or relating to this Contract or its

breach will be decided by arbitration if the parties mutually agree, or in a court of competent jurisdiction within the State in which the Agency is located.

Rights and Remedies

The duties and obligations imposed by the Contract documents and the rights and remedies available thereunder shall be in addition to and not a limitation of any duties, obligations, rights and remedies otherwise imposed or available by law. No action or failure to act by the Agency or Contractor shall constitute a waiver of any right or duty afforded any of them un